DefCon 22

Wireless Penetration Testing

and

How to WCTF

Sponsors!!!!!

W00T!!!

RF Pentesting Platforms

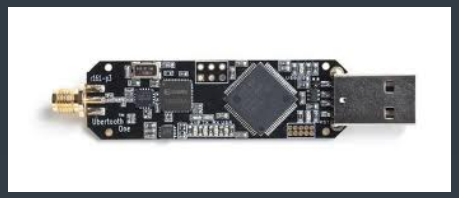
- Internet access
  - SmartPhone with USB tether (wifi/BT could be an issue)
- Laptop (MAC or PC)
  - Multi core processor
  - 8 GB ram or more* (16Gb+ optimal)
  - Hard drive space for all necessary apps and VMs
    - SSD is optimal
- External Radios/antennas
  - Internal radios might not give the flexibility/capability
  - Built in antennas may not give flexibility needed
- Power-Supply
  - Enough outlets to power all of your gear

RF Pentesting Distributions

- Pentoo
  - (bare metal, VM or overlay)
- Windows
  - (bare metal or VM)
- OS X with Fusion
  - Other Hosts with VM

RF Pentesting Radios

- Ubertooth One
- TP-Link TL-WN722N
- RTL-SDR
- Alfa Radios
- EnGenius EUB 1200AC
- Rokland N3
- Rosewill N600 UBE
- AirPcapNx
- HackRF Jawbreaker
- SR-71
- WiSpy DBX



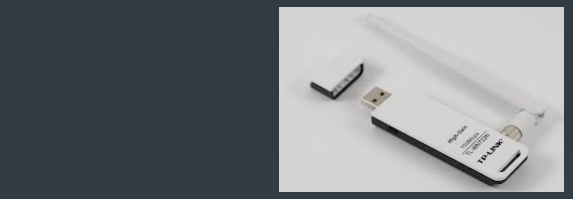


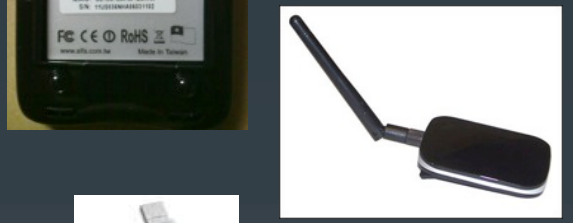





Get your ears up

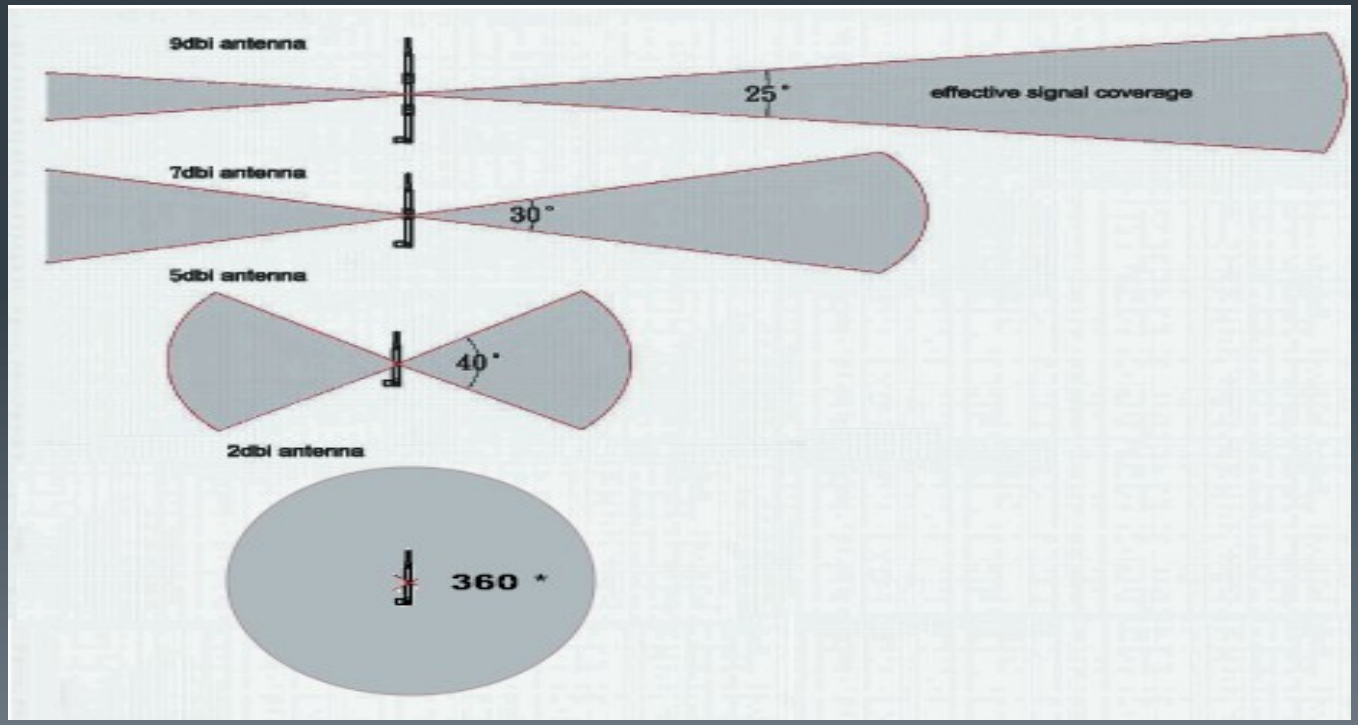
- There are thousands of headphones
- Headphones are a very personal decision
- They range in price and quality
- Find a pair that are comfortable and clear
- Types:
  - In ear
  - Over the ear (best)
  - On the ear





Antennas

- Omnidirectional
  - 2, 5, 7, 9 dBi
- Directional
  - Panel
  - Yagi
  - Cantena



RF Pentesting Tools

PGP/GPG
aircrack-ng
airodump-ng
airdrop-ng
kismet-ng
wireshark
tcpdump
nmap

msf
mdk3
reaver
pyrit
hashcat
wifite
fern-wifi-cracker
Smartnet-scanner

gqrx
multimon-ng
gnuradio
osmocom

SDR help needed???

- Listen to the speakers, ask questions, get an SDR and begin your journey
- Many of the SDR challenges give hints to the WiFi challenges
- We are RF loud and RF+ so please keep your ears up
- Someone on your team should have headphones

Testing Your Gear

- Have a repeatable process for validating antennas/setup
  - Hand testing on a fixed known AP
    - jitter.sh (ask we can give it to you
  - Automated testing Kismet (*shootout.rb*)
- Know how different cards, antennas, and combinations work with each platform

Never be surprised by your equipment

DefCon 22 WCTF

Down the Rabbit Hole

A True RF WCTF

WCTF Rules

- You must register with the scoring server
  - (instructions to follow)
- All “Game” BSSID’s are in the context of DCWCTF#
- Keys will only be scored once per team
- We log everything and obvious attempts will result in ***subjective*** penalties
  - We are much meaner than you :-p
- Anything that needs to be cracked will be that challenge’s key
  - If the AP is OPEN once connected, scan for a web server

offense and defense are always in play!

WCTF Scoring

- In order to score, you must have
  - A working copy of GPG or PGP depending on your operating system
  - A valid Public/Private key pair to be used for signing your submissions
  - Access to email/internet (internet is provided by DeFcon and maybe us)
- WCTF Scoring Instructions and PGP Public Key are at:

  http://PGP.wctf.us
- The flag.sh shell script has been provided to aid in uploading keys
- You will find that it makes it easier/faster to submit your scores

Setting up GPG/PGP

- Verify that you have PGP or GPG installed
  - Type gpg <return> and see if it is installed if not:
    - emerge gpg (Gentoo)
    - apt-get install gpg (Kali, Ubuntu, Debian, etc.)
    - Download and install GPG Keychain Access (OSX)

Setting up GPG/PGP keys

- From the terminal type Gpg –gen-key <return>
  - Select type (use default for WCTF)
  - Select keysize (use 1024 for WCTF)
  - Let the key expire a day after the WCTF is over
  - Type your “WCTF” name
  - Enter a valid email address that you are going to use to submit the flags for the WCTF
  - Enter a passphrase that you will remember
  - Then let the computer work for a few minutes creating entropy (wifi scanning speeds this process)

Register Your Team

http://wctf.us/register.php

Importing WCTF PGP Key

- gpg –import <paste the WCTF pub key> <return>
  - Copy/paste the entire key _only from
    - http://www.wctf.us/scoring.html

To Submit a Flag

- Copy the flag from it's location.
  - It will be either the wireless encryption key
  - A string of random characters found on the target network
  - On a web server on the target network
    - (nmap can be your friend nmap –p x.x.x.0/24
  - Copy the entire string with no breaks or spaces
  - If the key is hex convert to ASCII, remember to “ or ‘ when necessary
- Take the output of key.sh
  - ./flag.sh <flag>
- Copy and paste resulting output of the flag.sh file and email (without encryption) to: **ctf@wtcf.us**

WCTF Tactics

- Figure out the clues, and think hard
- The clues are always obscure and never direct
- Have a process or sequential processes to get through each challenge and follow that process!
- Take really good notes, either on paper or in a text file, I promise it will help

Flags

- There are 150 flags
- The flags have varying point values
- Submit as soon as you get your flags, some flags are depreciating

NEW this year…Offensive points

- There are 100 offensive flags
- All offense flags are worth ***-50 points***
- 4 flags will be given to the first 20 teams
- The staff have discretionary flags to give
- All of the staff but @rmellendick have flags to use
- These can be used as creatively as you want

BE EVIL!!!!

welcome to the challenges!

This will be edited on Aug 7th

Words, Context, Formatting, and Capitalization are all part of the clues

We are being very open this year

- Take a look at the equipment, but don't touch
- Understand the playing field cause it will change
- There are forces beyond our control (evil laugh) but well within your control
- Don't fall for the pit falls
- We are very open this year

- That is all

HINTS!!!!!

- Capture all the handshakes, many of the solutions will be evident later in the contest
- There is a need to find some of the solutions…somewhere else
- Keep track of everything
- Multitasking will help you succeed

Fox and Hound DCWCTFoxAndHound

- TP LINK ESSID: e8:94:f6:f3:d5:9a
- The fox will have the right to turn off the AP for up to 5 min per hour if it thinks it is in danger.
- The fox will be released before the village opens on Friday and will run till caught
- The “playing field”:
  - The RIO property
  - Parties
  - The entire hotel is in play ***EXCEPT*** the casino floor

##PRIZE##

A Reaver Pro, and additional 3 flags

Thanks to TNS

Hide and Seek DCWCTFHideAndSeek

- ESSID: 64:66:B3:E4:00:12
- The H&S will be running from Thursday morning till the con ends, the points are deprecating
- The target is stationary during the contest
- The “playing field”:
  - The RIO property
  - The entire hotel is in play ***EXCEPT*** the casino floor

##PRIZE##

A WiSpy Dbx and Channelizer 5
Thanks to METAGEEK

Challenge 1 WCTF

this may look easy but there is a catch

100 points

Challenge 2 WCTF

- You will have to be Direct to make this work
- 150 points

Challenge 3 WCTF

- Lol you got this
- 70 points

Challenge 4 WCTF

- Where did everyone go?
- 110 points

Challenge 5 WCTF

- Look to the air, and you will find me, I am hiding in plain sight
- 150 points

Challenge 6 WCTF

- Good luck wireshark is your friend, hints to follow
- 150 points

Challenge 7 WCTF

- Watch me if you can, then crack me if you can
- 150 points

Challenge 8 WCTF

- Look for this high and low, I am there
- 150 points

Challenge 9 WCTF

- Ping Pong, find the packet!
- 100 points

Challenge 10 WCTF

- This should be easy with some help, let it go, let it go
- 80 points

Challenge 11 WCTF

- This is a speed challenge, winner gets cool stuff
- 100 points, decreasing by 5 each time it is submitted

##PRIZE##

Challenge 12 WCTF

- This is like getting a coffee and hacking shit
- 100 points decreasing by 5 points

Challenge 13 WCTF

- This is to help boost motivation, but you will have to wait to get the answer…
- 150 points

Challenge 14 WCTF

- This is a nice break, but odd
- 40 points

Challenge 15 WCTF

- I love Steve, and so does my wonderful wife
- 130 points

Challenge 16 WCTF

- Another speed challenge, first to break, get cool prizes!!!!
- 100 points decreasing by 5 each time it is submitted

##PRIZE##

Challenge 17 WCTF

- This should be easy but esoteric
- 115 points

Challenge 18 WCTF

- Start at 80MHz and go up
- Deprecating

Challenge 19 WCTF

- Start at 50MHz and go up
- Deprecating

Challenge 20 WCTF

- Start at 215MHz and go up
- Deprecating

Challenge 21 WCTF

- Start at 144MHz and go up
- Deprecating

Challenge 22 WCTF

- Start at 900MHz and go up
- Deprecating

Challenge 23 WCTF

- Start at 5.8GHz and go up
- Deprecating

Challenge 24 WCTF

- Start at 900MHz and go up
- Deprecating

Challenge 25 WCTF

- Start at 73MHz and go up
- Deprecating

Challenge 26 WCTF

- Look for morse and find a president that can really fly

Challenge 27 WCTF

- following challenge 26 this will start to make sense, Mr Morse will guide you through it, but you might have to ask yourself…. hmmmm

Challenge 28 WCTF

- Actresses name
- 55 points

Challenge 29 WCTF

- This is in the form of a question, and is a picture.
- 55 points

Challenge 30 WCTF

- FFD8 to FFD9, and unzip

145 points

Challenge 31 WCTF

- SHA all the things
- 105 points

Challenge 32 WCTF

- Industrial Control networks
- 55 points

Challenge 33 WCTF

- The whole nmap syntax
- 55 points

Challenge 34 WCTF

- The whole sshnuke command
- 55 points

Challenge 35 WCTF

- Which building floors were shutdown?
- 55 points

Challenge 36 WCTF

- The title of the window; case sensitive
- 55 points

Challenge 37 WCTF

- Title of the window; case sensitive
- 55 points

Challenge 38 WCTF

- The system hostname
- 55 points

Challenge 39 WCTF

- The systems IP address; hack the wireless keyboard.
- 115 points

Challenge 40 WCTF

- Check the meta data of the digital stream. There is more than one answer
- 95 points

Challenge 41 WCTF

- Check the meta data in this digital stream; there is more than one answer.
- 95 points

Challenge 42 WCTF

- Dad jokes with modems.
- 55 points

Challenge 43 WCTF

- You'll have to xmit back to it; make sure you're legal ☺
- 55 points

Challenge 44 WCTF

- Play through the whole predictable xmit sequence. You can hop scotch through the answers without starting over.
- 55 points

Challenge 45 WCTF

- The motion detector on the wall's device ID. Manchester encoding and googling. No periods and lower case.
- 85 points

Challenge 46 WCTF

- Cell tower information
- 155 points

Challenge 47 WCTF

- POCSAG
- 225 points

Thanks to the WCTF Team

Anch	**TheX1le**
Marauder	***Zero_Chaos***
Terrible	***DntLookBehindu***
DaKahuna	***Dragorn***

Questions

@Rmellendick **rmellendick@gmail.com**